

PROFIL DE PROTECTION

ROUTEUR AVEC ÉLÉMENT DE CONFIANCE EMBARQUÉ

V4.0

Table des matières

Table des Tables

1 Introduction au Profil de Protection

Cette introduction au Profil de Protection (PP) est constituée de 4 paragraphes:

- Le paragraphe 1.1 introduit le document et fournit les références du présent Profil de Protection;
- Le paragraphe 1.2 énonce les références de la cible d'évaluation (TOE);
- Le paragraphe 1.3 donne une vue d'ensemble de la TOE destinée aux clients potentiels de la TOE;
- Le paragraphe 1.4 fournit plus de détails de la TOE, destiné plutôt aux rédacteurs de cible de sécurité, évaluateurs et certificateurs.

1.1 Identification du Profil de Protection (PP)

Alcatel-Lucent, Oppida, Telecom ParisTech, Telecom & Management SudParis, Trusted Labs et Trusted Logic se sont réunis au sein du groupe ESTER (**E**volution de la **S**écurité dans les **T**élécommunications et **E**quipements de **R**éseau) pour lancer une initiative visant à intégrer une base de confiance sur une carte à puce dans les éléments d'infrastructure du réseau afin d'en améliorer la protection. Ce projet a été financé par l'ANR (**A**gence **N**ationale de la **R**echerche).

Ce PP a été rédigé dans le cadre du projet ESTER et définit un ensemble d'objectifs et d'exigences de sécurité, indépendant de l'implémentation d'un routeur integrant une carte à puce.

Titre :	Profil de Protection, **R**outeur avec **É**lément de **C**onfiance **E**mbarqué[1]
Auteur :	Trusted Labs
Version :	4.0
Date :	8 décembre 2009
Référence :	PP RECE
Version des CC :	3.1 Révision 3

1.2 Vue d'ensemble de la TOE

La TOE est un nœud du réseau (un routeur) intégrant un module de sécurité (une carte à puce). Son rôle principal est l'acheminement des informations entre les différents nœuds du réseau d'une manière sécurisé.

Ce PP définit les exigences de sécurité, auxquelles la TOE doit se conformer en vue d'une évaluation de sécurité.

[1] Dans le reste du document le terme « **routeur ESTER** » désigne un « **routeur avec élément de confiance embarqué** (RECE)»

1.2.1 Utilisation de la TOE

L'infrastructure réseau comprend les éléments matériels qui permettent d'assurer la connexion des terminaux des utilisateurs par l'intermédiaire du réseau d'accès. Les fonctions de routage mises en œuvre dépendent du rôle du routeur dans l'infrastructure : routeur de bordure ou de cœur. Un domaine d'administration appelé aussi « système autonome » (AS) se définit comme une portion contigüe de l'internet contrôlée par une même autorité administrative. La frontière d'un tel domaine est marquée par les routeurs de bordure.

Un flot individuel consiste en une séquence de paquets issus d'un utilisateur. Ces flots sont agrégés selon les classes de services. On obtient alors des agrégats de flots. Cette architecture conduit à procéder à un ordonnancement des agrégats de flots au cœur du réseau et au contrôle des flots individuels en bordure.

La TOE est un nœud du réseau. C'est un routeur d'infrastructure intégrant une carte à puce et dont le rôle est de gérer le routage des flots individuels d'une manière sécurisée.

1.2.2 Type de TOE

La TOE est un produit composé des éléments matériels et logiciels suivants :

- un routeur;
- une carte à puce;
- l'application embarquée sur le routeur assurant les fonctionnalités de base pour lesquelles l'équipement est prévu;
- l'application ESTER embarquée sur la carte à puce.

1.2.3 Caractéristiques de sécurité de la TOE

Afin d'améliorer la sécurité des infrastructures réseau, notamment l'authentification des messages de gestion et de contrôle, la TOE comprend, en plus des fonctionnalités d'un routeur normal, une carte à puce. Celle-ci agissant comme un coffre-fort électronique protège les éléments sensibles (données de protocole, clés, ...) au sein même des nœuds de ces infrastructures.

Cette solution assure un environnement de confiance pour la génération, la protection des clés cryptographiques, la signature des messages en vue de leur authentification. Ce qui permet de se protéger contre des attaques visant à détruire et falsifier les éléments vitaux au fonctionnement du réseau.

La TOE assurera un niveau élevé de sécurité pour:

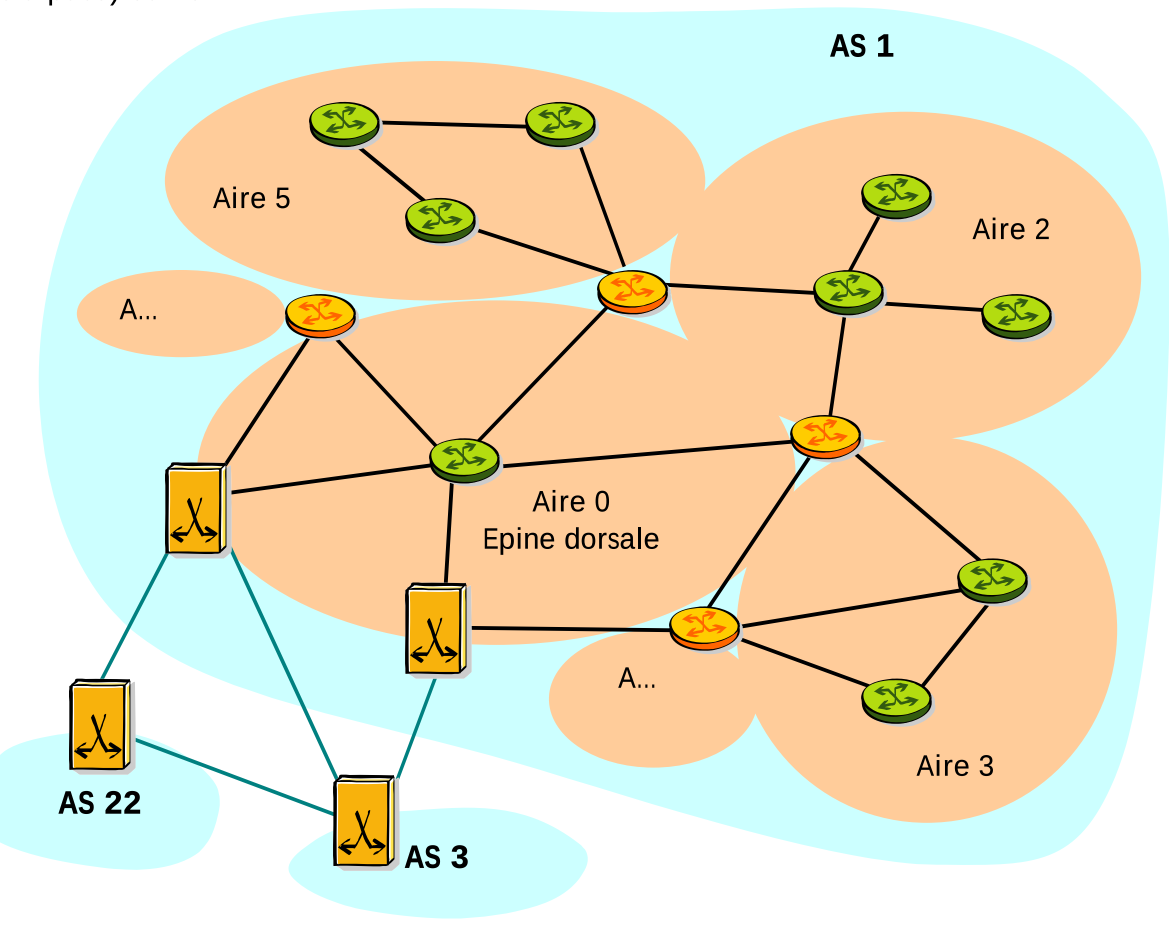
- l'infrastructure, en protégeant efficacement les protocoles de gestion et de contrôle (clés OSPF, tables de routage, ...)
- Le nœud lui-même, en permettant un mode minimal de sécurité où, même si le nœud a été attaqué et qu'il est sous contrôle complet de l'attaquant, certaines informations resteront secrètes et protégées par la carte à puce. Ceci afin d'éviter que l'attaque se propage vers les réseaux voisins.

1.2.4 Environnement de la TOE

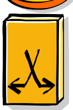
Un domaine d'administration, ou système autonome (AS), se définit comme une portion contiguë de l'Internet contrôlée par une même autorité administrative. La frontière d'un tel domaine est marquée par les routeurs de bordure.

Un système autonome, voir la Figure 1, possède un numéro d'identification de 1 à 65535. Ce numéro est géré au niveau international.

La TOE est un nœud d'un système autonome interagissant avec d'autres routeurs, qu'ils fassent partie du même AS ou non. Ces routeurs pourront être de type ESTER (routeur + carte à puce) ou non.



 Routeur d'aire

 Routeur de bordure d'aire

Routeur de bordure de système autonome (AS)

Figure 1: Composition des systèmes autonomes

1.3 Description de la TOE

1.3.1 Architecture générale de la TOE

La Figure 2 représente l'architecture d'un routeur ESTER avec ses différents plans.

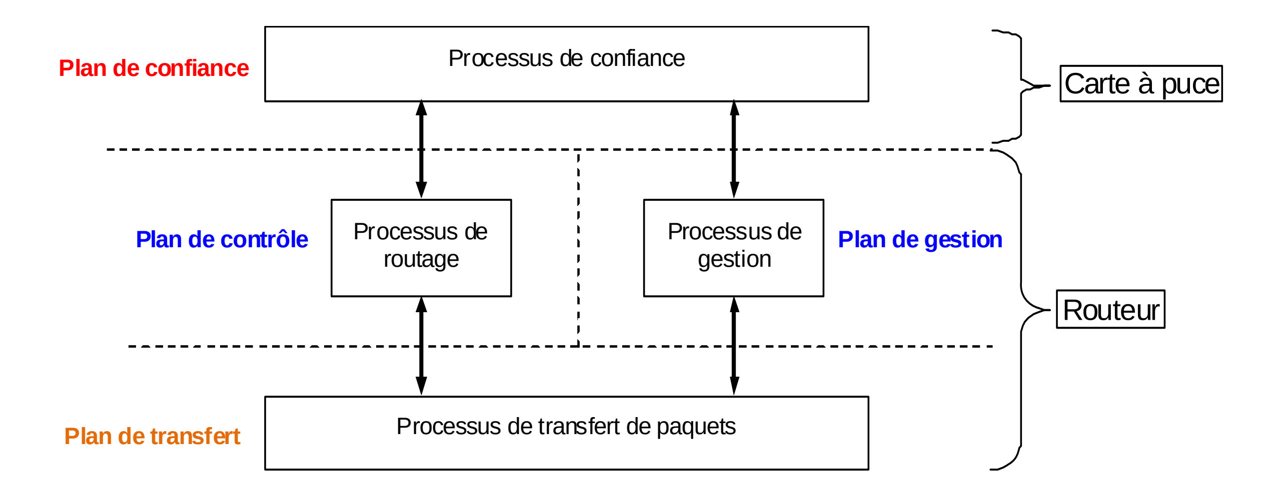


Figure 2: Les différents plans dans le cas d'un routeur

L'architecture d'un routeur repose sur une séparation logique des fonctionnalités supportées par l'équipement, lesquelles peuvent être réparties sur différents plans :

- **Plan de contrôle** ou **plan de commande** (*control plane*): il établit et maintient les tables de routage (RIB, Routing Information Base) qui sont mises à jour par l'intermédiaire d'échanges des protocoles de routages (OSPF, RIP, BGP,...). Il gère également les tables de labels (*LIB, Label Information Base*) dans le cas de MPLS. En ce qui concerne particulièrement le protocole OSPF, la mise à jour des LSAs, le calcul du chemin plus court (algorithme de Dijkstra), l'élaboration de la table de routage (RIB) et de la table d'aiguillage (FIB) sont localisés dans ce plan.

- **Plan de transfert** ou **plan de données** (*data plane*): il regroupe les fonctions de commutation à partir des tables d'aiguillage ou *forwarding* (*FIB, Forwarding Information Base ou LFIB, Label Forwarding Information Base*) pour l'acheminement des paquets IP ou MPLS. La FIB est l'agrégation des RIBs, des interfaces et des routes statiques configurées localement.

- **Plan de gestion** (*management plane*): contrôle notamment la configuration de l'élément de réseau, stocke et analyse différentes mesures provenant du réseau. Il inclut différents modules comme l'interface de commande en ligne (CLI), les connexions (Telnet, SSH), la supervision réseau (SNMP), etc.

Le routeur ESTER intègre une base de confiance protégée par une carte à puce dans les éléments d'infrastructure. Le terme de *base de confiance* est alors étendu à ***plan de confiance***.

Ce plan de confiance est intégré dans l'architecture définie par le groupe de travail IETF [ForCES] sous la forme d'un plan situé au niveau le plus haut, au-dessus des plans de contrôle de gestion. Il est chargé d'opérer le minimum de fonctions requises pour établir la confiance dans la sécurité du routeur tout particulièrement pour le protocole OSPF.

En effet, l'idée est d'éviter de propager une attaque aux routeurs voisins communicants avec le routeur ESTER par le biais du protocole OSPF et de la confiner au sein du routeur ESTER attaqué. Une fois le routeur ESTER corrompu, il est considéré comme n'étant plus de confiance et sera isolé du réseau.

1.3.2 Cycle de vie

Les cycles de vie du routeur et de la carte à puce suivent deux routes différentes avant l'intégration et la mise en opération. Ces deux processus seront protégées de deux manières différentes, la sensibilité des biens manipulés n'étant pas la même. Le routeur nécessite de ce fait une protection plus légère puisque les éléments sensibles seront stockés sur la carte. A contrario, celle-ci suivra un processus plus sécurisé, en utilisant une authentification à base de clés ou de codes PIN différents pour chacune des phases correspondant à chacun des intervenants sur la carte.

1.3.3 Rôles

Le fonctionnement de la TOE dans son environnement opérationnel fait appel directement ou indirectement aux rôles décrits ci-dessous.

Administrateur Réseau

Administrateur réseau du routeur ESTER. Son rôle est de définir la configuration du routeur par défaut, de monter un tunnel sécurisé avec la carte, consulter le mode courant de la carte, monter un tunnel sécurisé avec le routeur, consulter les logs et modifier la configuration du routeur.

Administrateur de sécurité

Administrateur local de sécurité du routeur ESTER. Son rôle est de définir la politique de sécurité par défaut de la TOE, de monter un tunnel sécurisé avec la carte, consulter le mode courant de la carte, modifier le mode courant de la carte, mettre à jour les clés et les certificats, définir les événements à tracer et d'analyser les événements d'audit concernant la gestion du routeur.

Opérateur

Opérateur du routeur. Son rôle est d'assurer le bon fonctionnement du routeur ESTER dans l'infrastructure du réseau tant que les conditions de sécurité restent réunies (en assurant par exemple la remise en route suite à une coupure de courant). Il est responsable du maintien en condition opérationnelle de la TOE dans le système d'information au sein duquel elle se trouve.

Utilisateur

Les utilisateurs du routeur sont les routeurs voisins qui communiquent avec la TOE. Un utilisateur a pour rôle d'envoyer et de recevoir des messages OSPF.

Superviseur

Superviseur (local ou distant) du routeur ESTER. Son rôle est de vérifier le bon fonctionnement du routeur, monter un tunnel sécurisé avec la carte, consulter le mode courant de la carte, consulter les logs et recevoir des traps SNMP.

Dans la suite du document, le rôle **Administrateur** regroupe les rôles: **Administrateur de sécurité** et **Administrateur Réseau**.

1.4 Limites de la TOE

Cette section distingue précisément ce qui est inclus dans la TOE, qui sera donc évalué, de ce qui fait partie de son environnement opérationnel.

1.4.1 Architecture physique

La Figure 3 présente un exemple d'architecture physique envisageable pour la TOE.



Figure 3. Exemple d'architecture physique de la TOE.

Il faut noter que le lecteur de carte à puce ne fait pas parti de la TOE et appartient donc à son environnement opérationnel.

1.4.2 Architecture logique

La Figure 2 présente un exemple des composants fonctionnels qui constituent la TOE au niveau logique.

Une partie du processus de traitement ou de la pile OSPF (trusted part) est déportée sur le plan de confiance dont l'implémentation est réalisée par une carte à puce. La partie restante sur le routeur est appelée de non-confiance (untrusted part).

La partie de la pile OSPF « trusted » communique avec la partie de la pile OSPF « untrusted » par l'intermédiaire de l'interface de communication « Smart Card Comm. Interface ». Ce canal n'est pas sécurisé.

Le plan de confiance dispose d'un certain nombre de librairies et d'interfaces (API) afin d'assurer des fonctionnalités cryptographiques et autres (e.g. Crypto API, GP API, etc.)

Le plan de confiance peut garder des traces de certaines opérations ou actions dans sa base de « Filtered logs » et peut stocker des informations sensibles (clés, certificats, etc.) y sont

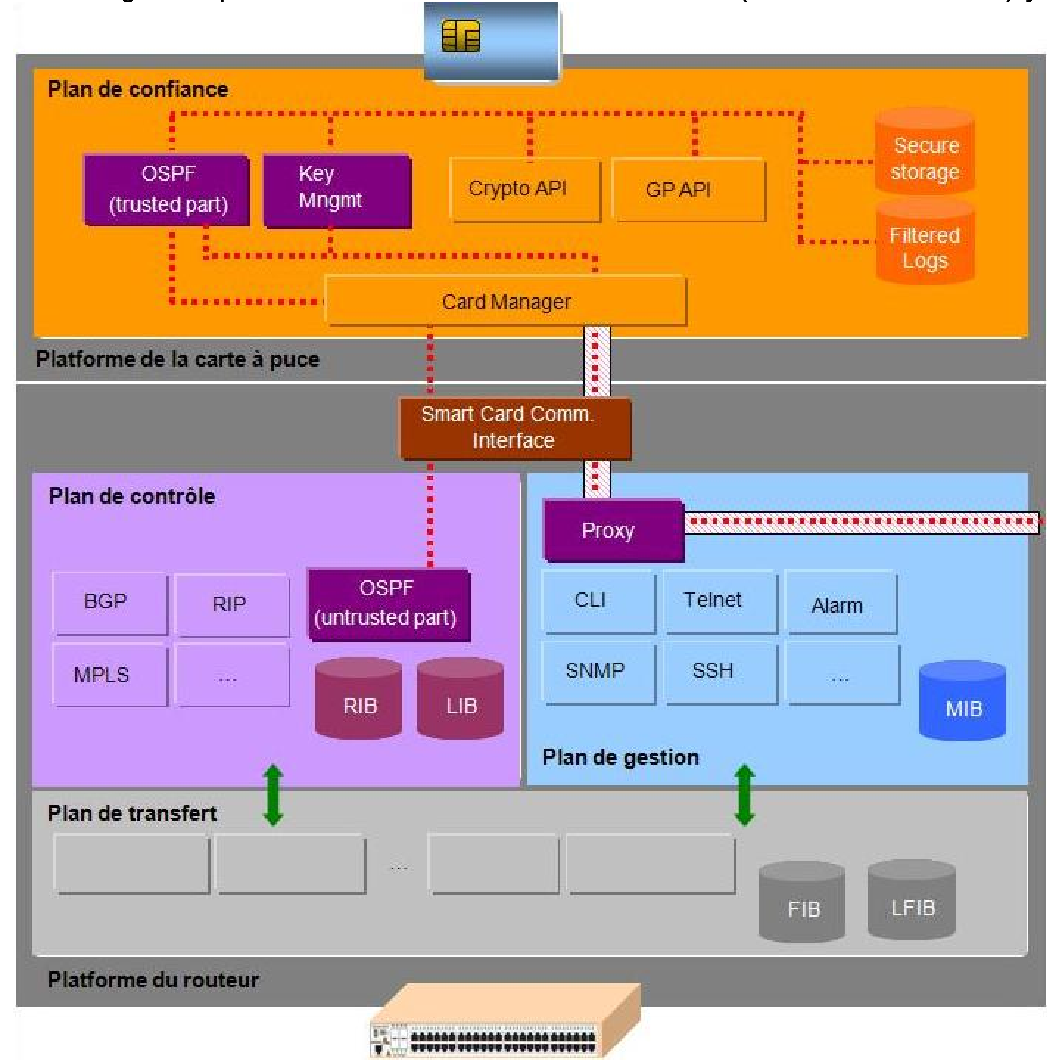


Figure 4: Architecture logique de la TOE

1.5 Environnement opérationnel de la TOE

Pour la sécurité de la TOE, les routeurs ESTER et les équipements d'administration doivent se trouver dans un endroit sûr et leurs accès doivent être contrôlés. L'administration à distance du routeur ESTER et la supervision du routeur ESTER est possible via une station distante.

1.5.1 Le Gestionnaire de Sécurité

L'architecture logique de la TOE nécessite un gestionnaire de sécurité qui est principalement en charge d'assurer la gestion des clés et des certificats, de leur génération, de leur mise à jour, etc. Celui-ci fait parti de l'environnement opérationnel de la TOE.

Le gestionnaire communique directement avec la carte à puce via un canal sécurisé. Un proxy est nécessaire sur le routeur pour assurer cette communication sécurisée de bout en bout. Ce gestionnaire possède une interface graphique de gestion pour effectuer des actions décrites dans la section 1.2.1 : *Utilisation de la TOE*.

Les modules « Key Mngmt » dans le gestionnaire et dans la carte à puce interagissent pour la gestion des clés et certificats.

1.6 Définitions

Un glossaire donnant la définition des principaux termes utilisés dans la suite du document est fourni en Annexe A.

1.7 Acronymes

AC	**Autorité de Certification**
API	Application Programming Interface
AS	Système Autonome
CC	(*Common Criteria*) Critères Communs
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
GP	Global Platform
IP	Internet Protocol
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
PP	Profil de Protection
SNMP	Simple Network Management Protocol
TOE	Target of Evaluation

1.8 Références

[CC1]	**Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, Revision 3, July 2009.**
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements. Version 3.1, Revision 3, July 2009.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, Revision 3, July 2009.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, Revision 3, July 2009.
[ForCES]	http://www.ietf.org/html.charters/forces-charter.html

2 Déclarations de conformité

Ce chapitre contient les sections suivantes :

Déclaration de conformité aux CC (2.1)

Déclaration de conformité à un Paquet (2.2)

Déclaration de conformité du PP (2.3)

Déclaration de conformité au PP (2.4)

2.1 Déclaration de conformité aux CC

Ce profil de protection est conforme aux Critères Communs version 3.1.

Ce PP a été écrit conformément aux CC version 3.1:

- CC Partie 1 [CC1]
- CC Partie 2 [CC2]
- CC Partie 3 [CC3]
- CEM [CEM]

Aucune interprétation ou extension aux parties 2 et 3 n'a été retenue.

2.2 Déclaration de conformité à un Paquet

Le niveau d'assurance d'évaluation (EAL) est **EAL1** augmenté de **ADV_ARC.1, AVA_VAN.2, ADV_TDS.1**, **ADV_FSP.2, ASE_OBJ.2, ASE_REQ.2 et ASE_SPD.1.**

2.3 Déclaration de conformité du PP

Ce PP ne déclare de conformité à aucun autre PP.

2.4 Déclaration de conformité au PP

La conformité retenue dans ce PP pour les Cibles de Sécurité et Profils de Protection qui s'y déclarent conformes est la conformité **démontrable** selon la définition dans la Partie 1 des CC [CC1].

3 Définition du problème de sécurité

3.1 Biens

Les biens sensibles à protéger par la TOE sont les suivants:

Paquet de routage

Les paquets OSPF de routage qui transitent entre les différents noeuds du réseau. Ces paquets contiennent l'information nécessaire dont le routeur à besoin pour accomplir sa fonction de routage.

Localisation: carte à puce et routeur

Protection: intégrité

Table de routage

La table de routage comporte des informations sur l'aiguillage des messages afin d'atteindre un équipement ou un réseau donné.

Localisation: routeur et carte à puce

Protection: intégrité

Clés privées

Ensemble des clés cryptographiques privées utilisées par le plan de confiance pour assurer la communication sécurisée entre la TOE et la station d'administration. Ces clés permettent le déchiffrement et la création de signature.

Localisation: carte à puce

Protection: intégrité, confidentialité

Clés publiques

Ensemble des clés cryptographiques publiques utilisées par le plan de confiance pour assurer la communication sécurisée entre la TOE et la station d'administration. Ces clés permettent le chiffrement et la vérification de signature.

Localisation: routeur et carte à puce

Protection: intégrité

Secrets

Les clés partagées, les mots de passe et les PIN codes pour s'identifier auprès de la TOE et avoir accès à des fonctionnalités spécifiques (administrateurs).

Localisation: carte à puce

Protection: intégrité, confidentialité

Audits

Les audits représentent les fichiers contenant les informations sur les derniers événements liés au fonctionnement du routeur.

Localisation: routeur

Protection: intégrité, confidentialité

Note d'application:

La localisation des biens sensibles à protéger par la TOE dépendra de l'implémentation du produit final (routeur ESTER). C'est au rédacteur de la cible de sécurité se conformant à ce PP de préciser la localisation exacte de chaque bien sensible dans les composants de la TOE.

3.2 Menaces

Les agents menaçants peuvent être:

des utilisateurs "autorisés" de la TOE (les utilisateurs qui ont des droits prédéfinis d'utilisation de la TOE comme les administrateurs par example);

ou des utilisateurs "non autorisés" de la TOE.

Lorsqu'une menace provient soit des utilisateurs autorisés ou non autorisés, ceux-ci sont considérés comme des attaquants.

Les attaquants sont censés avoir différents niveaux d'expertise, de motivation et des ressources. Leur expertise pourrait couvrir la génie logiciel, l'administration réseau, les routeurs, le "hacking", etc.

En effet, la TOE peut faire l'objet de nombreuses menaces qui touchent à la confidentialité et l'intégrité de ses données et services. Ces attaques peuvent être de nature physique ou logique.

3.2.1 Menaces liés à la compromission des informations

M.ECOUTE_COM

Un attaquant capture et analyse les données qui transitent entre les éléments de la TOE, afin de récupérer les données d'authentification ou d'autres informations sensibles et rejouer ces messages d'authentification pour avoir un accès inapproprié aux données sensibles ou configurer la TOE d'une façon inappropriée. Ce qui peut ouvrir la porte aux attaques ciblant le routeur.

M.DIVULG_CLES

Un attaquant parvient à accéder sur le système-cible aux clés secrètes utilisées pour protéger les données et les rend publiques. Ce qui entraine une perte d'image et de crédibilité de l'opérateur liée à la perte de données sensibles. Cela peut aussi causer une perte financière liée à la génération et la redistribution d'une nouvelle clé.

M.USURPATION_ID

Un attaquant usurpe l'identité d'un utilisateur autorisé afin d'accéder aux données sensibles et de récupérer les données d'identification ou d'authentification.

M.PIEGEAGE_PATCH

Un attaquant parvient à partir du mécanisme de mise-à-jour de la TOE à y installer un logiciel d'écoute ou de contrôle. La plupart des données contenues ou manipulées par le routeur deviennent potentiellement accessibles et modifiables (Clés, données d'authentification, les fichiers logs, etc).

3.2.2 Menaces liés aux défaillances techniques

M.DYSFONCTION_ROUTEUR

Le routeur ne fonctionne plus correctement soit à cause d'une panne éventuelle ou d'un acte de malveillance d'un utilisateur. Ce qui cause une perturbation du service et une perte financière liée à la réparation ou au remplacement du routeur.

M.DYSFONCTION_CARTE

La carte à puce liée au routeur ne fonctionne plus correctement soit à cause d'une panne éventuelle ou d'un acte de malveillance d'un utilisateur. Ce qui peut compromettre les fonctions de sécurité du routeur et une perte financière liée à la réparation ou au remplacement de la carte.

M.OBSOLETE

Le système d'exploitation ou le logiciel du routeur ou de la carte à puce ne sont plus au niveau pour assurer les fonctions exigées.

3.2.3 Menaces liés aux actions illicites

M.UTIL_ILLICITE

Un opérateur en dehors des phases de contrôle ou un utilisateur non autorisé utilise le système-cible, notamment pour l'accès aux informations secrètes.

M.ALTER_CLES

Un attaquant parvient à modifier les clés stockées dans la TOE.

M.ALTER_LOGS

Un attaquant parvient à modifier les journaux d'événements stockés dans la TOE.

M.ALTER_TABLE_DE_ROUTAGE

Un attaquant parvient à modifier la table de routage stockée dans la TOE.

M.ALTER_NSC

Un attaquant parvient à modifier le numéro de séquence cryptographique stocké sur la carte.

M.ALTER_PAQUET_DE_ROUTAGE

Un attaquant parvient à modifier les paquets de routage qui transitent entre les différents noeuds du réseau.

3.2.4 Menaces liés à la compromission des fonctions

M.ADMIN_ERREUR

Un administrateur peut commettre une fausse installation ou une fausse configuration de la TOE. Il est possible aussi qu'il installe une TOE corrompue entrainant l'inefficacité des mécanismes de sécurité.

M.USURPATION_FORCE

Un attaquant profite de la faiblesse du système d'authentification pour casser par force brute l'accès à la TOE.

Note d'application:

Le système d'authentification repose sur MD5 qui est l'algorithme d'authentification standard de OSPF.

M.RENIEMENT_CONTROLE

Un attaquant renie avoir utilisé le routeur pour l'accès aux informations sensibles.

M.RENIEMENT_CONFIG

Un attaquant renie avoir utilisé le routeur pour des finalités de configuration.

3.3 Politiques de sécurité organisationnelles (OSP)

P.ETIQUETTE

La cible d'évaluation doit afficher une étiquette décrivant des restrictions d'utilisation, les accords légaux, ou n'importe quelle autre information appropriée à laquelle les utilisateurs consentent en accédant à la TOE.

P.COMPATIBILITE

La TOE doit rester compatible avec les normes et les protocoles courants et futurs. L'intégration du composant de sécurité doit être le plus possible transparente vis-à-vis de l'infrastructure.

P.ACCES_ADMIN

Les administrateurs doivent avoir la possibilité d'administrer la TOE à distance ou sur place. Cette communication doit être effectuée par des canaux sécurisés.

P.ETAT_DE_L'ART

Les exigences sur la carte et sur l'interface avec le routeur doivent être en accord avec les performances des systèmes existants. Ils doivent aussi suivre l'état de l'art des technologies réseaux.

3.4 Hypothèses

H.ATTAQUE_PHYSIQUE

Le système cible est placé, en phase d'usage, dans des locaux conçus pour assurer sa protection contre toutes attaques physiques sur la carte ou le routeur. Par exemple, la carte à puce ne peut pas être retirée brutalement du routeur en fonction.

H.MESURES_DE_SECURITE

Des procédures traitant de mesures techniques, physiques, organisationnelles et liées aux personnels quant à la confidentialité et à l'intégrité du matériel, du logiciel et des informations propriétaires du concepteur de la TOE doivent exister et être appliquées pendant la phase d'usage du cycle de vie de la TOE.

Note d'application:

Ces mesures de sécurité ne concernent pas "toutes les phases du cycle de vie de la TOE", mais seulement les phases liées à la partie opérationnelle.

H.SERVICES

La fourniture des services essentiels au fonctionnement des matériels (électricité, réseau) est assurée, de bonne qualité et maîtrisée.

H.EVOLUTION

L'organisation s'assure de la pérennité des solutions en regard de l'état de l'art et de l'évolution du système d'information.

H.LECTEUR

Le lecteur de carte à puce fait parti de l'environnement opérationnel de la TOE. Il est considéré de confiance.

4 Objectifs de sécurité

4.1 Objectifs de sécurité pour la TOE

O.ROLE_ADMIN

La TOE doit fournir des fonctionnalités d'administrateur qui seront capables d'isoler les actions administratives et d'effectuer des fonctions administratives localement et à distance d'une manière sécurisé.

O.CRYPTO

La TOE doit fournir des fonctionnalités cryptographiques (cryptage / décryptage et la signature numérique) performantes et sécurisées.

O.ACCES_ROBUSTE

La TOE doit fournir des mécanismes qui contrôlent l'accès logique des utilisateurs et d'interdire l'accès à des utilisateurs spécifiques le cas échéant.

O.AUTHENTIFICATION_ADMIN

La TOE doit authentifier les administrateurs afin de les affectés les rôles correspondants.

O.MODE_REACTION

En réponse à la détection d'une attaque, la TOE doit réagir pour éviter de propager les données corrompues aux routeurs voisins.

O.GESTION

La TOE doit fournir toutes les fonctionnalités et les installations qui facilitent la tâche aux administrateurs dans leur gestion de la sécurité tout en fournissant une restriction d'accès pour des utilisateurs non autorisés.

O.MISE_A_JOUR

Des mécanismes de sécurité doivent être mis en place pour protéger les données sensibles pendant leur mis à jour.

O.MISE_A_JOUR_LOGICIEL

Des mises à jour régulières des logiciels doivent être faites. Celles-ci ne doivent dégrader ni la sécurité, ni les fonctionnalités des versions antérieures.

O.AUDIT_INTEGRITE

L'intégrité des fichiers de log enregistrées et manipulées par la TOE doit être garantie.

O.AUDIT_ALERT

La TOE doit fournir des moyens pour alerter l'administrateur lors de la détection d'une violation de potentielle de la TOE.

O.REJEU

La TOE doit fournir un moyen de détection et de refus du rejeu de l'authentification et d'autres messages sensibles.

4.2 Objectifs de sécurité pour l'environnement opérationnel

OE.SERVICES

La fourniture des services essentiels au fonctionnement des matériels (électricité, réseau) doit être assurée, de bonne qualité et maîtrisée.

OE.SURVEILLANCE_LOG

Pour tout système, il doit être possible de détecter en temps réel ou a posteriori un comportement anormal, de retracer les opérations réalisées et d'identifier les auteurs.

OE.MOTS_DE_PASSE

L'organisation doit s'assurer de la bonne gestion (changements réguliers) et de l'utilisation de mots de passe de l'opérateur suffisamment robustes.

OE.INTEGRITE_MAT

L'organisation doit contrôler l'intégrité et l'authenticité du routeur et de la carte.

OE.ADMIN_SECRET

L'administrateur doit être sensibilisé au respect du secret professionnel et de la discrétion.

OE.EVOLUTION

L'organisation doit s'assurer de la pérennité des solutions en regard de l'état de l'art et de l'évolution du système d'information.

OE.REDONDANCE

L'organisation doit assurer le remplacement immédiat du routeur ou de la carte en cas de panne.

OE.LOCAUX

Les locaux où se trouve le routeur ESTER doivent être protégés contre toute menace physique.

OE.CYCLE_DE_VIE

Des procédures doivent assurer la protection du matériel, du logiciel et des informations de la TOE pendant la phase d'usage du cycle de vie de la TOE. Elles comprennent les objectifs suivants:

- Protection physique contre les dommages externes
- Procédures sécurisés de manipulation et de stockage
- Traçabilité des TOE en cours de livraison
- Non-divulgation des informations relatives à la sécurité
- Identification des éléments à livrer,

- Respect des règles de confidentialité

Note d'application:

Ces mesures de sécurité ne concernent pas "toutes les phases du cycle de vie de la TOE", mais seulement les phases liées à la partie opérationnelle.

OE.PROTOCOLES

L'opérateur doit s'assurer de la conformité des protocoles implémentés avec la norme standard et les spécifications de l'industrie pour garantir l'interopérabilité du routeur.

OE.AFFICHAGE_ETIQUETTE

La TOE doit afficher une étiquette indiquant un avertissement sur le mode d'emploi de la TOE.

OE.LECTEUR

Le lecteur de carte à puce doit être évaluer et attester conforme à une norme de sécurité reconnue à l'échelle mondiale.

4.3 Argumentaire des objectifs de sécurité

4.3.1 Menaces

4.3.1.1 Menaces liés à la compromission des informations

M.ECOUTE_COM Cette menace est couverte par les objectifs de sécurité suivants:

- O.CRYPTO qui permet de chiffrer les données sensibles transitant entre les éléments de la TOE;
- OE.MOTS_DE_PASSE qui assure que les mots de passe utilisés par l'opérateur pour s'authentifier auprès de la TOE sont robustes et renouvelés régulièrement.

Cette menace est aussi couverte par l'objectif O.REJEU qui assure une détection et un refus des messages rejoués.

M.DIVULG_CLES Cette menace est couverte par les objectifs suivants:

- O.CRYPTO qui fournit des fonctionnalités cryptographiques performantes protégeant les clés secrètes contre la divulgation;
- O.MISE_A_JOUR qui assure des mécanismes de sécurité lors de la mise à jour des clés secrètes
- OE.MOTS_DE_PASSE qui assure que les mots de passe utilisés par l'opérateur pour s'authentifier auprès de la TOE sont robustes et renouvelés régulièrement;
- OE.ADMIN_SECRET qui assure que l'administrateur est sensibilisé au respect du secret professionnel et de la discrétion.

M.USURPATION_ID Cette menace est couverte par les objectifs suivants:

- O.ROLE_ADMIN qui permet de fournir des fonctionnalités d'administrateur qui seront capables d'isoler les actions administratives et d'effectuer des fonctions administratives localement et à distance de manière sécurisée

- O.CRYPTO qui fournit des fonctionnalités cryptographiques performantes protégeant contre l'usurpation d'identité
- O.REJEU qui assure que la TOE détectera et refusera toute tentative de rejeu des données d'identification usurpées
- O.MODE_REACTION qui assure que la TOE est capable de réagir pour contrer l'attaque et éviter de propager les données corrompues aux routeurs voisins
- O.MISE_A_JOUR qui assure des mécanismes de sécurité lors de la mise à jour des données sensibles et ainsi ne pas permettre une usurpation d'identité lors du processus d'authentification
- OE.MOTS_DE_PASSE qui assure que les mots de passe utilisés par l'opérateur pour s'authentifier auprès de la TOE sont robustes et renouvelés régulièrement
- O.AUTHENTIFICATION_ADMIN qui assure qu'un administrateur s'est bien authentifié avant de se connecter au routeur
- O.ACCES_ROBUSTE qui assure que la TOE possède un système de contrôle d'accès logique interdisant l'accès à un attaquant souhaitant usurper l'identité d'un utilisateur autorisé.

M.PIEGEAGE_PATCH Cette menace est couverte par les objectifs suivants:

- O.MISE_A_JOUR qui garanti que les fonctions de sécurité de la TOE permettent de protéger les données sensibles lors de leur mis à jour
- O.MISE_A_JOUR_LOGICIEL qui assure que les logiciels mis à jour n'ont aucun impact sur la sécurité de la TOE

4.3.1.2 Menaces liés aux défaillances techniques

M.DYSFONCTION_ROUTEUR Cette menace est couverte par les objectifs de sécurité suivants:

- OE.INTEGRITE_MAT qui garantit que les procédures administratives contrôlent l'intégrité et l'authenticité du routeur pour éviter tout dysfonctionnement
- OE.REDONDANCE qui assure que le routeur sera remplacé immédiatement par un autre en cas de dysfonctionnement
- OE.LOCAUX qui assure que les locaux où se trouve le routeur sont bien sécurisés contre tout type de menace physique.

M.DYSFONCTION_CARTE Cette menace est couverte par les objectifs de sécurité suivants:

- O.AUDIT_ALERT qui alerte l'administrateur lors de la détection d'un dysfonctionnement de la carte
- O.MODE_REACTION qui assure que la TOE est capable de réagir à cette menace et éviter de propager les données corrompues aux routeurs voisins
- OE.INTEGRITE_MAT qui garanti que les procédures administratives contrôlent l'intégrité et l'authenticité de la carte pour éviter tout dysfonctionnement
- OE.REDONDANCE qui assure que la carte sera remplacée immédiatement par une autre en cas de dysfonctionnement

- OE.LOCAUX qui assure que les locaux où se trouve la TOE sont bien sécurisés contre tout type de menace physique.

M.OBSOLETE Cette menace est couverte par les objectifs de sécurité suivants:

- O.MISE_A_JOUR_LOGICIEL qui assure que la version de l'OS et des logiciels de la TOE sont mis à jour pour fournir les fonctions exigées;
- OE.EVOLUTION qui assure que les procédures administratives assureront la pérennité des solutions technologiques de la TOE en regard de l'état de l'art et de l'évolution du système d'information.

4.3.1.3 Menaces liés aux actions illicites

M.UTIL_ILLICITE Cette menace est couverte par les objectifs de sécurité suivants:

- O.ACCES_ROBUSTE qui assure que la TOE possède un mécanisme de contrôle d'accès logique interdisant l'accès à un attaquant.

M.ALTER_CLES Cette menace est couverte par les objectifs suivants:

- O.CRYPTO qui permet de chiffrer les données sensibles de la TOE dans le but de protéger les clés cryptographiques;
- O.MISE_A_JOUR qui assure des mécanismes de sécurité lors de la mise à jour des clés secrètes;
- O.MODE_REACTION qui assure que la TOE est capable de réagir pour contrer l'attaque et éviter de propager les données corrompues aux routeurs voisins;
- O.AUDIT_ALERT qui alerte l'administrateur lors de la détection d'une altération des clés;
- O.AUTHENTIFICATION_ADMIN qui assure qu'un administrateur s'est bien authentifié avant de se connecter au routeur;

M.ALTER_LOGS Cette menace est couverte par les objectifs suivants:

- O.AUDIT_INTEGRITE qui garanti que les logs sont protégés en intégrité;
- O.MODE_REACTION qui assure que la TOE est capable de réagir pour contrer l'attaque et éviter de propager les données corrompues aux routeurs voisins;
- O.AUDIT_ALERT qui alerte l'administrateur lors de la détection d'une altération des logs.

M.ALTER_TABLE_DE_ROUTAGE Cette menace est couverte par les objectifs suivants:

- O.CRYPTO qui fournit des mécanismes cryptographiques permettant de garantir l'intégrité des paquets de routage;
- O.AUDIT_ALERT qui alerte l'administrateur lors de la détection d'une altération des paquets de routage.

M.ALTER_NSC Cette menace est couverte par les objectifs suivants:

- O.CRYPTO qui permet de chiffrer les données sensibles de la TOE dans le but de protéger les clés cryptographiques;
- O.MODE_REACTION qui assure que la TOE est capable de réagir pour contrer l'attaque et éviter de propager les données corrompues aux routeurs voisins;

- O.MISE_A_JOUR qui assure des mécanismes de sécurité lors de la mise à jour des clés secrètes.
- O.AUDIT_ALERT qui alerte l'administrateur lors de la détection d'une altération du NSC.

M.ALTER_PAQUET_DE_ROUTAGE Cette menace est couverte par les objectifs suivants:

- O.CRYPTO qui fournit des mécanismes cryptographiques permettant de garantir l'intégrité des tables de routage;
- O.MISE_A_JOUR qui assure des mécanismes de sécurité lors de la mise à jour des tables de routage;
- O.AUDIT_ALERT qui alerte l'administrateur lors de la détection d'une altération de la table de routage.
- O.MODE_REACTION qui assure que la TOE est capable de réagir pour contrer l'attaque et éviter de propager les paquets de routage corrompues aux routeurs voisins;

4.3.1.4 Menaces liés à la compromission des fonctions

M.ADMIN_ERREUR Cette menace est couverte par les objectifs suivants:

- O.GESTION qui assure que la TOE fournit toutes les fonctionnalités et les installations qui facilitent la tâche aux administrateurs dans leur gestion de la sécurité tout en fournissant une restriction d'accès pour des utilisateurs non autorisés.

M.USURPATION_FORCE Cette menace est couverte par les objectifs suivants:

- O.CRYPTO qui assure que les fonctions de sécurité de la TOE fournissent des mécanismes de sécurité à base de clés cryptographiques garantissant un haut niveau de sécurité;
- OE.MOTS_DE_PASSE qui assure que les mots de passe utilisés par l'opérateur pour s'authentifier auprès de la TOE sont robustes et renouvelés régulièrement;
- O.MODE_REACTION qui assure que la TOE est capable de réagir pour contrer l'attaque et éviter de propager les données corrompues aux routeurs voisins.
- O.ACCES_ROBUSTE qui assure que la TOE possède un système de contrôle d'accès logique interdisant l'accès à un attaquant souhaitant casser par force brute l'accès à la TOE.

M.RENIEMENT_CONTROLE Cette menace est couverte par les objectifs suivants:

- O.AUDIT_INTEGRITE qui garantit que les logs sont protégés en intégrité
- O.AUTHENTIFICATION_ADMIN qui assure qu'un administrateur s'est bien authentifié avant de se connecter au routeur
- OE.SURVEILLANCE_LOG qui permet de retracer les opérations réalisées et d'identifier les auteurs.

M.RENIEMENT_CONFIG Cette menace est couverte par les objectifs suivants:

- O.AUDIT_INTEGRITE qui garanti que les logs sont protégés en intégrité;

- O.AUTHENTIFICATION_ADMIN qui assure qu'un administrateur s'est bien authentifié avant de se connecter au routeur;
- OE.SURVEILLANCE_LOG qui permet de retracer les opérations réalisées et d'identifier les auteurs.

4.3.2 Politiques de sécurité organisationnelles (OSP)

P.ETIQUETTE Cette politique de sécurité organisationnelle est couverte par l'objectif de sécurité sur l'environnement OE.AFFICHAGE_ETIQUETTE garantissant qu'une étiquette indiquant un avertissement sur le mode d'emploi de la TOE doit être affichée clairement sur la TOE.

P.COMPATIBILITE Cette politique de sécurité organisationnelle est couverte par l'objectif de sécurité sur l'environnement OE.PROTOCOLES qui assure une conformité des protocoles implémentés avec la norme standard et les spécifications de l'industrie pour garantir l'interopérabilité du routeur.

P.ACCES_ADMIN Cette politique de sécurité organisationnelle est couverte par les objectifs de sécurité O.ROLE_ADMIN et O.AUTHENTIFICATION_ADMIN qui garantissent une administration sécurisé de la TOE. De plus, l'objectif O.ACCES_ROBUSTE assure que la TOE possède un système de contrôle d'accès logique garantissant un accès privilégié aux administrateurs.

P.ETAT_DE_L'ART Cette politique de sécurité organisationnelle est couverte par l'objectif de sécurité sur l'environnement OE.EVOLUTION qui garantie que l'organisation en charge de la TOE doit s'assurer de la pérennité des solutions en regard de l'état de l'art et de l'évolution du système d'information.

4.3.3 Hypothèses

H.ATTAQUE_PHYSIQUE Cette hypothèse est couverte par le l'objectif de sécurité OE.LOCAUX assurant que la TOE se trouve dans des locaux sécurisés.

H.MESURES_DE_SECURITE Cette hypothèse est couverte par l'objectif de sécurité sur l'environnement OE.CYCLE_DE_VIE qui garantie l'existence des procédures assurant la protection du matériel, du logiciel et des informations de la TOE tout le long de son cycle de vie.

H.SERVICES Cette hypothèse est couverte par l'objective de sécurité sur l'environnement OE.SERVICES qui assure que la fourniture des services essentiels au fonctionnement des matériels est assurée, de bonne qualité et maîtrisée.

H.EVOLUTION Cette hypothèse est couverte par l'objectif de sécurité sur l'environnement OE.EVOLUTION qui garantie que l'organisation en charge du routeur doit s'assurer de la pérennité des solutions en regard de l'état de l'art et de l'évolution du système d'information.

H.LECTEUR Cette hypothèse est confirmée par l'objective de sécurité sur l'environnement de la TOE OE.LECTEUR qui guaranti que le lecteur de carte à puce doit être évaluer et attester conforme à une norme de sécurité reconnue à l'échelle mondiale.

4.3.4 Tables de couverture entre définition du problème et objectifs de sécurité

Menaces	Objectifs de sécurité	Argumentaire
M.ECOUTE_COM	O.CRYPTO, OE.MOTS_DE_PASSE, O.REJEU	Section 4.3.1
M.DIVULG_CLES	O.CRYPTO, O.MISE_A_JOUR, OE.MOTS_DE_PASSE, OE.ADMIN_SECRET	Section 4.3.1
M.USURPATION_ID	O.ROLE_ADMIN, O.CRYPTO, O.MODE_REACTION, O.MISE_A_JOUR, OE.MOTS_DE_PASSE, O.AUTHENTIFICATION_ADMIN, O.REJEU, O.ACCES_ROBUSTE	Section 4.3.1
M.PIEGEAGE_PATCH	O.MISE_A_JOUR, O.MISE_A_JOUR_LOGICIEL	Section 4.3.1
M.DYSFONCTION_ROUTEUR	OE.REDONDANCE, OE.LOCAUX, OE.INTEGRITE_MAT	Section 4.3.1
M.DYSFONCTION_CARTE	OE.REDONDANCE, OE.LOCAUX, OE.INTEGRITE_MAT, O.AUDIT_ALERT, O.MODE_REACTION	Section 4.3.1
M.OBSOLETE	O.MISE_A_JOUR_LOGICIEL, OE.EVOLUTION	Section 4.3.1
M.UTIL_ILLICITE	O.ACCES_ROBUSTE	Section 4.3.1
M.ALTER_CLES	O.CRYPTO, O.MISE_A_JOUR, O.AUTHENTIFICATION_ADMIN, O.MODE_REACTION, O.AUDIT_ALERT	Section 4.3.1
M.ALTER_LOGS	O.MODE_REACTION, O.AUDIT_ALERT, O.AUDIT_INTEGRITE	Section 4.3.1
M.ALTER_TABLE_DE_ROUTAGE	O.CRYPTO, O.AUDIT_ALERT	Section 4.3.1
M.ALTER_NSC	O.CRYPTO, O.MODE_REACTION, O.MISE_A_JOUR, O.AUDIT_ALERT	Section 4.3.1
M.ALTER_PAQUET_DE_ROUTAGE	O.CRYPTO, O.MISE_A_JOUR, O.AUDIT_ALERT, O.MODE_REACTION	Section 4.3.1
M.ADMIN_ERREUR	O.GESTION	Section 4.3.1
M.USURPATION_FORCE	O.CRYPTO, O.ACCES_ROBUSTE, O.MODE_REACTION, OE.MOTS_DE_PASSE	Section 4.3.1
M.RENIEMENT_CONTROLE	O.AUDIT_INTEGRITE, OE.SURVEILLANCE_LOG, O.AUTHENTIFICATION_ADMIN	Section 4.3.1
M.RENIEMENT_CONFIG	O.AUDIT_INTEGRITE, OE.SURVEILLANCE_LOG, O.AUTHENTIFICATION_ADMIN	Section 4.3.1

Table 1 Association menaces vers objectifs de sécurité

Objectifs de sécurité	Menaces
O.ROLE_ADMIN	M.USURPATION_ID
O.CRYPTO	M.ECOUTE_COM, M.DIVULG_CLES, M.USURPATION_ID, M.ALTER_CLES, M.ALTER_TABLE_DE_ROUTAGE, M.ALTER_NSC, M.ALTER_PAQUET_DE_ROUTAGE, M.USURPATION_FORCE
O.ACCES_ROBUSTE	M.USURPATION_ID, M.UTIL_ILLICITE, M.USURPATION_FORCE
O.AUTHENTIFICATION_ADMIN	M.USURPATION_ID, M.ALTER_CLES, M.RENIEMENT_CONTROLE, M.RENIEMENT_CONFIG
O.MODE_REACTION	M.USURPATION_ID, M.DYSFONCTION_CARTE, M.ALTER_CLES, M.ALTER_LOGS, M.ALTER_NSC, M.ALTER_PAQUET_DE_ROUTAGE, M.USURPATION_FORCE
O.GESTION	M.ADMIN_ERREUR
O.MISE_A_JOUR	M.DIVULG_CLES, M.USURPATION_ID, M.PIEGEAGE_PATCH, M.ALTER_CLES, M.ALTER_NSC, M.ALTER_PAQUET_DE_ROUTAGE
O.MISE_A_JOUR_LOGICIEL	M.PIEGEAGE_PATCH, M.OBSOLETE
O.AUDIT_INTEGRITE	M.ALTER_LOGS, M.RENIEMENT_CONTROLE, M.RENIEMENT_CONFIG
O.AUDIT_ALERT	M.DYSFONCTION_CARTE, M.ALTER_CLES, M.ALTER_LOGS, M.ALTER_TABLE_DE_ROUTAGE, M.ALTER_NSC, M.ALTER_PAQUET_DE_ROUTAGE
O.REJEU	M.ECOUTE_COM, M.USURPATION_ID
OE.SERVICES	
OE.SURVEILLANCE_LOG	M.RENIEMENT_CONTROLE, M.RENIEMENT_CONFIG
OE.MOTS_DE_PASSE	M.ECOUTE_COM, M.DIVULG_CLES, M.USURPATION_ID, M.USURPATION_FORCE
OE.INTEGRITE_MAT	M.DYSFONCTION_ROUTEUR, M.DYSFONCTION_CARTE
OE.ADMIN_SECRET	M.DIVULG_CLES
OE.EVOLUTION	M.OBSOLETE
OE.REDONDANCE	M.DYSFONCTION_ROUTEUR,

Objectifs de sécurité	Menaces
	M.DYSFONCTION_CARTE
OE.LOCAUX	M.DYSFONCTION_ROUTEUR, M.DYSFONCTION_CARTE
OE.CYCLE_DE_VIE	
OE.PROTOCOLES	
OE.AFFICHAGE_ETIQUETTE	
OE.LECTEUR	

Table 2 Association objectifs de sécurité vers menaces

Politiques de sécurité organisationnelles (OSP)	Objectifs de sécurité	Argumentaire
P.ETIQUETTE	OE.AFFICHAGE_ETIQUETTE	Section 4.3.2
P.COMPATIBILITE	OE.PROTOCOLES	Section 4.3.2
P.ACCES_ADMIN	O.ROLE_ADMIN, O.AUTHENTIFICATION_ADMIN, O.ACCES_ROBUSTE	Section 4.3.2
P.ETAT_DE_L'ART	OE.EVOLUTION	Section 4.3.2

Table 3 Association politiques de sécurité organisationnelles vers objectifs de sécurité

Objectifs de sécurité	Politiques de sécurité organisationnelles (OSP)
O.ROLE_ADMIN	P.ACCES_ADMIN
O.CRYPTO	
O.ACCES_ROBUSTE	P.ACCES_ADMIN
O.AUTHENTIFICATION_ADMIN	P.ACCES_ADMIN
O.MODE_REACTION	
O.GESTION	
O.MISE_A_JOUR	
O.MISE_A_JOUR_LOGICIEL	
O.AUDIT_INTEGRITE	
O.AUDIT_ALERT	
O.REJEU	
OE.SERVICES	
OE.SURVEILLANCE_LOG	
OE.MOTS_DE_PASSE	
OE.INTEGRITE_MAT	
OE.ADMIN_SECRET	
OE.EVOLUTION	P.ETAT_DE_L'ART
OE.REDONDANCE	
OE.LOCAUX	
OE.CYCLE_DE_VIE	
OE.PROTOCOLES	P.COMPATIBILITE
OE.AFFICHAGE_ETIQUETTE	P.ETIQUETTE
OE.LECTEUR	

Table 4 Association objectifs de sécurité vers politiques de sécurité organisationnelles

Hypothèses	Objectifs de sécurité pour l'environnement opérationnel	Argumentaire
H.ATTAQUE_PHYSIQUE	OE.LOCAUX	Section 4.3.3
H.MESURES_DE_SECURITE	OE.CYCLE_DE_VIE	Section 4.3.3
H.SERVICES	OE.SERVICES	Section 4.3.3
H.EVOLUTION	OE.EVOLUTION	Section 4.3.3
H.LECTEUR	OE.LECTEUR	Section 4.3.3

Table 5 Association hypothèses vers objectifs de sécurité pour l'environnement opérationnel

Objectifs de sécurité pour l'environnement opérationnel	Hypothèses
OE.SERVICES	H.SERVICES
OE.SURVEILLANCE_LOG	
OE.MOTS_DE_PASSE	
OE.INTEGRITE_MAT	
OE.ADMIN_SECRET	
OE.EVOLUTION	H.EVOLUTION
OE.REDONDANCE	
OE.LOCAUX	H.ATTAQUE_PHYSIQUE
OE.CYCLE_DE_VIE	H.MESURES_DE_SECURITE
OE.PROTOCOLES	
OE.AFFICHAGE_ETIQUETTE	
OE.LECTEUR	H.LECTEUR

Table 6 Association objectifs de sécurité pour l'environnement opérationnel vers hypothèses

5 Exigences de sécurité

5.1 Exigences de sécurité fonctionnelles

5.1.1 Audit and security alerts

FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **the following actions:**

- **alert the administrator**
- **and audit events**

upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **[selection: choose one of: minimum, basic, detailed, not specified]** level of audit; and

c) **[assignment: other specifically defined auditable events]**.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: other audit relevant information]**.

FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of **[assignment: subset of defined auditable events]** known to indicate a potential security violation;

b) **[assignment: any other rules]**.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **the audit administrator** with the capability to read **[assignment: list of audit information]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.2 Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to **detect** unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that **[assignment: metric for saving audit records]** stored audit records will be maintained when the following conditions occur: **audit storage exhaustion, failure and attack**

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application note: These SFRs apply to the router and/or the smart card components depending on the product's implementation.

5.1.2 ESTER Router management

5.1.2.1 Cryptographic operations

FCS_COP.1 / Data encryption / decryption Cryptographic operation

FCS_COP.1.1 / Data encryption / decryption The TSF shall perform **data encryption / decryption** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

FCS_COP.1 / MAC generation Cryptographic operation

FCS_COP.1.1 / MAC generation The TSF shall perform **MAC generation** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

FCS_COP.1 / Hashing Cryptographic operation

FCS_COP.1.1 / Hashing The TSF shall perform **hash generation** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

FCS_COP.1 / RNG Cryptographic operation

FCS_COP.1.1 / RNG The TSF shall perform **random number generation** in accordance with a specified cryptographic algorithm **[assignment: cryptographic algorithm]** and cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application note:

These SFRs apply to the smart card.

5.1.2.2 Key management

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application note:

This SFR applies to the smart card.

5.1.2.3 Key destruction

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

Application note:

This SFR applies to the smart card.

5.1.3 Identification and authentication

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within [assignment: range of acceptable values]** unsuccessful authentication attempts occur related to

- **Administrator's authentication**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[selection: met, surpassed]**, the TSF shall **block the communication with the card**.

FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note:

These SFRs apply to the router and/or the smart card components depending on the product's implementation.

5.1.4 Security management

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **determine the behaviour of, enable, modify the behaviour of and disable** the functions

- **Security Audit (FAU_SAR.1, FAU_SAR.2)**
- **Security Audit Analysis (FAU_SAA.1)**
- **Security Alarms (FAU_ARP.1)**

to **Audit Administrator**.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **[selection: change_default, query, modify, delete, clear, [assignment: other operations]]** the **[assignment: list of TSF data]** to **Security Administrator**.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[assignment: list of management functions to be provided by the TSF]**.

Application note:

The editor of the Security Target that complies with this PP shall describe each management function and to which administrator this function is provided.

FMT_SMR.2 / Administrator role Restrictions on security roles

FMT_SMR.2.1 / Administrator role The TSF shall maintain the roles:

- **Security Administrator role,**
- **Network Administrator role,**
- **Audit Administrator role**.

FMT_SMR.2.2 / Administrator role The TSF shall be able to associate users with roles.

FMT_SMR.2.3 / Administrator role The TSF shall ensure that the conditions **[assignment: conditions for the different roles]** are satisfied.

Application note:

The TOE administration is limited to the capabilities associated with an administrative role.

Application note:

These SFRs apply to the router and/or the smart card components depending on the product's implementation.

5.1.5 Protection of the TSF

FPT_RPL.1 Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities:

- **authentication data**.

FPT_RPL.1.2 The TSF shall perform

- **reject routing paquets,**
- **audit event,**
- ***selection: [assignment: list of specific actions], none]]***

when replay is detected.

Application note:

This SFR applies to the smart card.

5.1.6 Trusted Path / Channels

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- **creation of cryptographic keys (shared keys, assymetric keys,...)**

- **update of cryptographic keys**.

FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure**.

FTP_TRP.1.2 The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial user authentication and [assignment: other services for which trusted path is required]**.

Application note:

These SFRs apply to the smart card.

5.1.7 Conclusion

Application note :

Subjects, objects, operations, security attributes are not defined in this PP because they are not used in the SFRs and the SARs. The security target writer shall define these elements in case they are used in an SFR that has been added to the original set of SFRs defined in this PP.

5.2 Exigences de sécurité d'assurance

Le niveau des exigences d'assurance de sécurité est EAL1 augmenté de ADV_ARC.1, AVA_VAN.2, ADV_TDS.1, ADV_FSP.2, ASE_OBJ.2, ASE_REQ.2 et ASE_SPD.1.

5.3 Argumentaire des exigences de sécurité

5.3.1 Objectifs

5.3.1.1 Objectifs de sécurité pour la TOE

O.ROLE_ADMIN Cet objectif est couvert par l'exigence de sécurité FMT_SMR.2/ Administrator role qui assure que l'utilisateur humain doit être affecté à un ou plusieurs rôles d'administrateur (Sécurité, Réseaux et Audit) et les fonctions de sécurité affectés à chaque rôle sont isolées.

O.CRYPTO Cet objectif est couvert par toutes les exigences concernant la gestion des clés cryptographiques et les opérations cryptographiques: FCS_COP.1/ Data encryption/decryption, FCS_COP.1/ MAC generation, FCS_COP.1/ Hashing, FCS_COP.1/ RNG, FCS_CKM.1, FCS_CKM.4.

O.ACCES_ROBUSTE Cet objectif est couvert par FIA_UID.2 et FIA_UAU.2 qui exigent l'identification et l'authentification des Administrateurs (Réseaux, Sécurité et Audit) avant d'effectuer toute opération d'administration. De plus, cet objectif est également couvert par FMT_SMR.2/ Administrator role qui demande le maintien des différents rôles par la TOE suivant des conditions précises et par FIA_AFL.1 qui limite le nombre de fausses authentifications de l'administrateur avant de passer en mode réaction.

O.AUTHENTIFICATION_ADMIN Cet objectif est couvert par FIA_UID.2 et FIA_UAU.2 qui exigent l'identification et l'authentification des Administrateurs (Réseaux, Sécurité et Audit) avant d'effectuer toute opération d'administration. Cet objectif est également couvert par FMT_SMR.2/ Administrator role qui demande le maintien des différents rôles par la TOE suivant des conditions précises.

O.MODE_REACTION Cet objectif est couvert par l'éxigence de sécurité FAU_ARP.1 qui alerte les TSF lors de détection d'une violation potentielle de la TOE afin de réagir et blocker l'accès à la carte. Cet objectif est également couvert par les éxigences de sécurité FAU_GEN.1,FAU_GEN.2, FAU_SAA.1, FAU_SAR.1et FPT_STM.1 qui détectent et enregistre des évenements improbables liés au fonctionnement de la TOE dans des fichiers de logs pour ensuite pouvoir tracer l'attaque. L'éxigence de sécurité FPT_RPL.1 assure que les TSF peuvent détecter et réagir aux attaques de rejeu en rejetant les paquets de routages et enregistrer les évenements dans des logs.

O.GESTION Cet objectif est couvert par les exigences de sécurités fonctionnelles:

- FMT_MOF.1 qui fournit à l'administrateur d'audit les fonctionnalités spécifiques.
- FMT_MTD.1 qui fournit des fonctions de sécurité restrictives aux administrateurs de sécurité.

- FMT_SMF.1 qui spécifie les fonctionnalités qui doivent être fournies aux administrateurs de la TOE.

O.MISE_A_JOUR Cet objectif est couvert par

- FIA_UID.2 et FIA_UAU.2 qui exigent l'identification et l'authentification des Administrateurs (Réseaux, Sécurité et Audit) avant d'effectuer toute opération d'administration.
- FTP_TRP.1 qui impose un chemin de confiance avec l'Administrateur lors de la mise à jour des attributs de sécurité.
- FTP_ITC.1 qui exige l'implémentation d'un canal sécurisé assurant l'origine de l'administration du routeur et de la carte.

O.MISE_A_JOUR_LOGICIEL Cet objectif est couvert par:

- FTP_ITC.1 qui exige l'implémentation d'un canal sécurisé assurant l'origine de l'administration du routeur et de la carte
- FTP_TRP.1 qui impose un chemin de confiance avec l'Administrateur lors de la mise à jour des logiciels.

O.AUDIT_INTEGRITE Cet objectif est couvert par FMT_MOF.1 qui spécifie les fonctionnalités qui doivent être fournies aux administrateurs de la TOE. De plus cet objectif est couvert par FAU_STG.2 qui assure l'intégrité des fichiers d'audit enregistrés dans la TOE.

O.AUDIT_ALERT Cet objectif est couvert par lés exigences de sécurité FAU_ARP.1et FAU_SAR.1 qui alertent les TSF lors d'une detection de violation potentielle de la TOE et permet à l'administrateur d'audit de lire les fichiers d'audit. Les règles de détection sont définies dans FAU_SAA.1.

O.REJEU Cet objectif est couvert par l'éxigence de sécurité FPT_RPL.1 qui assure que les messages d'authentification des paquets de routages sont protégés contre les attaques de rejeu. Les TSF peuvent détecter et réagir en rejetant les paquets de routages.

5.3.2 Tables de couverture entre objectifs et exigences de sécurité

Objectifs de sécurité	Exigences fonctionnelles pour la TOE	Argumentaire
O.ROLE_ADMIN	FMT_SMR.2/ Administrator role	Section 5.3.1
O.CRYPTO	FCS_COP.1/ Data encryption/decryption, FCS_COP.1/ MAC generation, FCS_COP.1/ Hashing, FCS_COP.1/ RNG, FCS_CKM.1, FCS_CKM.4	Section 5.3.1
O.ACCES_ROBUSTE	FIA_UID.2, FIA_UAU.2, FIA_AFL.1, FMT_SMR.2/ Administrator role	Section 5.3.1
O.AUTHENTIFICATION_ADMIN	FIA_UAU.2, FIA_UID.2, FMT_SMR.2/ Administrator role	Section 5.3.1
O.MODE_REACTION	FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1, FPT_STM.1, FPT_RPL.1	Section 5.3.1
O.GESTION	FMT_MOF.1, FMT_MTD.1, FMT_SMF.1	Section 5.3.1
O.MISE_A_JOUR	FIA_UID.2, FTP_ITC.1, FTP_TRP.1, FIA_UAU.2	Section 5.3.1
O.MISE_A_JOUR_LOGICIEL	FTP_ITC.1, FTP_TRP.1	Section 5.3.1
O.AUDIT_INTEGRITE	FAU_STG.2, FMT_MOF.1	Section 5.3.1
O.AUDIT_ALERT	FAU_ARP.1, FAU_SAR.1, FAU_SAA.1	Section 5.3.1
O.REJEU	FPT_RPL.1	Section 5.3.1

Table 7 Association objectifs de sécurité de la TOE vers les exigences fonctionnelles

Exigences fonctionnelles pour la TOE	Objectifs de sécurité
FAU_ARP.1	O.MODE_REACTION, O.AUDIT_ALERT
FAU_GEN.1	O.MODE_REACTION
FAU_GEN.2	O.MODE_REACTION
FAU_SAA.1	O.MODE_REACTION, O.AUDIT_ALERT
FAU_SAR.1	O.MODE_REACTION, O.AUDIT_ALERT
FAU_STG.2	O.AUDIT_INTEGRITE
FPT_STM.1	O.MODE_REACTION
FCS_COP.1/ Data encryption/decryption	O.CRYPTO
FCS_COP.1/ MAC generation	O.CRYPTO
FCS_COP.1/ Hashing	O.CRYPTO
FCS_COP.1/ RNG	O.CRYPTO
FCS_CKM.1	O.CRYPTO
FCS_CKM.4	O.CRYPTO
FIA_AFL.1	O.ACCES_ROBUSTE
FIA_UAU.2	O.ACCES_ROBUSTE, O.AUTHENTIFICATION_ADMIN, O.MISE_A_JOUR
FIA_UID.2	O.ACCES_ROBUSTE, O.AUTHENTIFICATION_ADMIN, O.MISE_A_JOUR
FMT_MOF.1	O.GESTION, O.AUDIT_INTEGRITE
FMT_MTD.1	O.GESTION
FMT_SMF.1	O.GESTION
FMT_SMR.2/ Administrator role	O.ROLE_ADMIN, O.ACCES_ROBUSTE, O.AUTHENTIFICATION_ADMIN
FPT_RPL.1	O.MODE_REACTION, O.REJEU
FTP_ITC.1	O.MISE_A_JOUR, O.MISE_A_JOUR_LOGICIEL
FTP_TRP.1	O.MISE_A_JOUR, O.MISE_A_JOUR_LOGICIEL

Table 8 Association exigences fonctionnelles vers objectifs de sécurité de la TOE

5.3.3 *Dépendances*

5.3.3.1 Dépendances des exigences de sécurité fonctionnelles

Exigences	Dépendances CC	Dépendances Satisfaites
FAU_ARP.1	(FAU_SAA.1)	FAU_SAA.1
FAU_GEN.1	(FPT_STM.1)	FPT_STM.1
FAU_GEN.2	(FAU_GEN.1) et (FIA_UID.1)	FAU_GEN.1, FIA_UID.2
FAU_SAA.1	(FAU_GEN.1)	FAU_GEN.1
FAU_SAR.1	(FAU_GEN.1)	FAU_GEN.1
FAU_STG.2	(FAU_GEN.1)	FAU_GEN.1
FPT_STM.1	Pas de dépendance	
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.2
FIA_UAU.2	(FIA_UID.1)	FIA_UID.2
FIA_UID.2	Pas de dépendance	
FMT_MOF.1	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.2/ Administrator role
FMT_MTD.1	(FMT_SMF.1) et (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.2/ Administrator role
FMT_SMF.1	Pas de dépendance	
FMT_SMR.2/ Administrator role	(FIA_UID.1)	FIA_UID.2
FPT_RPL.1	Pas de dépendance	
FTP_ITC.1	Pas de dépendance	
FTP_TRP.1	Pas de dépendance	
FCS_COP.1/ Data encryption/decryption	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/ MAC generation	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_COP.1/ Hashing	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	
FCS_COP.1/ RNG	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2) et (FCS_CKM.4)	
FCS_CKM.1	(FCS_CKM.2 ou FCS_COP.1) et (FCS_CKM.4)	FCS_COP.1/ Data encryption/decryption, FCS_COP.1/ MAC generation, FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 ou FDP_ITC.1 ou FDP_ITC.2)	FCS_CKM.1

Table 9 Dépendances des exigences fonctionnelles

Argumentaire pour les dépendances non satisfaites

La dépendance FCS_CKM.4 de FCS_COP.1/ Hashing n'est pas supportée.

- La fonction de hachage ne requiert pas des clés cryptographiques.

La dépendance FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 de FCS_COP.1/ Hashing n'est pas supportée.

- La fonction de hashage ne nécessite ni la génération ni l'importation de clés dans la TOE.

La dépendance FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 de FCS_COP.1/ RNG n'est pas supportée.

- Le RNG ne necessite ni la génération ni l'importation de clés dans la TOE.

La dépendance FCS_CKM.4 de FCS_COP.1/ RNG n'est pas supportée.

- Le RNG ne requiert pas des clés cryptographiques.

5.3.3.2 Dépendances des exigences de sécurité d'assurance

Exigences	Dépendances CC	Dépendances Satisfaites
ADV_FSP.2	(ADV_TDS.1)	ADV_TDS.1
ADV_ARC.1	(ADV_FSP.1) et (ADV_TDS.1)	ADV_FSP.2, ADV_TDS.1
ADV_TDS.1	(ADV_FSP.2)	ADV_FSP.2
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.2
AGD_PRE.1	Pas de dépendance	
ALC_CMC.1	(ALC_CMS.1)	ALC_CMS.1
ALC_CMS.1	Pas de dépendance	
ASE_CCL.1	(ASE_ECD.1) et (ASE_INT.1) et (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	Pas de dépendance	
ASE_INT.1	Pas de dépendance	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) et (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_TSS.1	(ADV_FSP.1) et (ASE_INT.1) et (ASE_REQ.1)	ADV_FSP.2, ASE_INT.1, ASE_REQ.2
ASE_SPD.1	Pas de dépendance	
ATE_IND.1	(ADV_FSP.1) et (AGD_OPE.1) et (AGD_PRE.1)	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1
AVA_VAN.2	(ADV_ARC.1) et (ADV_FSP.2) et (ADV_TDS.1) et (AGD_OPE.1) et (AGD_PRE.1)	ADV_FSP.2, ADV_ARC.1, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

Table 10 Dépendances des exigences d'assurance

5.3.4 Argumentaire pour les exigences de sécurité d'assurance

Les augmentations rajoutées au niveau d'évaluation EAL1 visent à fournir une meilleure couverture des attaques potentielles. Cet objectif sera atteint en assurant que les audits de vulnérabilité et des tests de pénétration se basent sur les documents de conception basique et et d'architecture de sécurité, en plus des spécifications fonctionnelles plus détaillées.

5.3.5 ADV_ARC.1 Security architecture description

La sélection du composant ADV_ARC.1 est nécessaire afin de fournir suffisamment de données sur l'architecture de sécurité, pour effectuer les analyses de vulnérabilités.

5.3.6 AVA_VAN.2 Vulnerability analysis

La sélection du composant AVA_VAN.2 est nécessaire afin d'étendre la couverture de l'analyse des vulnérabilités et des tests de pénétration.

5.3.7 ADV_TDS.1 Basic design

La sélection du composant ADV_TDS.1 est nécessaire afin de fournir suffisamment de données de conception, en particulier les fonctions de sécurité "SFR-enforcing", pour effectuer l'analyse des vulnérabilités.

5.3.8 ADV_FSP.2 Security-enforcing functional specification

La sélection du composant ADV_FSP.2 est nécessaire afin de fournir des spécifications fonctionnelles avec suffisamment de détails, pour effectuer l'analyse des vulnérabilités.

5.3.9 ASE_OBJ.2 Security objectives

La séléction du composant ASE_OBJ.2 est nécessaire pour l'évaluation de la cible de sécurité se conformant à ce PP afin de fournir les argumentaires de couvertures des menaces, OSP et des hypohtèses par les objectifs de sécurité.

5.3.10 ASE_REQ.2 Derived security requirements

La séléction du composant ASE_REQ.2 est nécessaire pour l'évaluation de la cible de sécurité se conformant à ce PP afin de fournir les argumentaires de couvertures des objectifs de sécurité par les SFR.

5.3.11 ASE_SPD.1 Security problem definition

La séléction du composant ASE_SPD.1 est nécessaire pour l'évaluation de la cible de sécurité se conformant à ce PP afin de décrire les menaces, les OSP et les hypothèses s'appliquants à l'environement opérationel de la TOE.

6 Notice

Ce document a été généré avec TL SET version 2.3.6 (for CC3). Pour plus d'informations sur l'outil d'édition sécuritaire de Trusted Labs consultez le site internet www.trusted-labs.com.

Glossaire

Cette annexe définie les principaux termes utilisés dans ce document. Pour la définition des termes Critères Communs, se référer à [CC1], §4.

Terme	Déscription
Administrateur	Rôle endossé par une personne responsable d'une ou de plusieurs opérations sur un routeur ESTER. Ses tâches peuvent être l'installation, le paramétrage, le maintien, la mise à jour des matériels ou des logiciels liés à la TOE. Le terme « administrateur » utilisé dans le PP désigne les trois rôles d'administrateurs: administrateur de sécurité, administrateur de réseaux et administrateur d'audit.
Plan de confiance	Notion introduite dans ce projet qui représente le plan dans lequel s'exécute le minimum des fonctions critiques à la sécurité d'un équipement ou d'une architecture.
Plan de contrôle	Contient les fonctionnalités établissant et maintenant les bases d'information qui sont mises à jour par l'intermédiaire d'échanges entre fonctionnalités de ce plan des équipements voisins.
Plan de gestion	Contient les fonctionnalités qui concernent la configuration de l'élément de réseau.
Plan de transfert	Contient les fonctionnalités appliquant la synthèse des bases d'informations du plan contrôle et de gestion au trafic de données du réseau.

Index